IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Goodman et al.	:	Before the Examiner: Lipman, Jacob
Serial No.: 09/931,550	:	Group Art Unit: 2434
Filing Date: August 16, 2001	:	
Title: SYSTEM MANAGEMENT INTERRUPT GENERATION UPON COMPLETION OF CRYPTOGRAPHIC OPERATION	:	Lenovo (United States) Inc. Building 675, Mail C-137 4401 Silicon Drive Durham, NC 27709

REPLY BRIEF UNDER 37 C.F.R. §41.41

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Reply Brief is being submitted in response to the Examiner's Answer dated October 27, 2009, with a two-month statutory period for response set to expire on December 27, 2009.

I. RESPONSE TO EXAMINER'S ARGUMENTS:

A. Response to Examiner's assertion that Examiner provided an appropriate motivation for modifying Alexander with Grawrock to include the missing claim limitation of claims 4 and 13, as discussed on pages 7 and 8 of Examiner's Answer.

Most if not all inventions arise from a combination of old elements. *See In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Obviousness is determined from the vantage point of a hypothetical person having ordinary skill in the art to which the patent pertains. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Therefore, an Examiner may often find every element of a claimed invention in the prior art. *Id.* However, identification in the prior art of each individual part claimed is insufficient to defeat patentability of the whole claimed invention. *See Id.* In order to establish a *prima facie* case of obviousness, the Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998). The Examiner must provide articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (cited approvingly in *KSR International Co. v. Teleflex Inc.*, 82 U.S.P.Q.2d 1385, 1396 (U.S. 2007)).

The Examiner admits that Alexander does not teach that the verifying step is performed by a trusted platform module in accordance with the Trusted Computing Platform Alliance Specifications, as recited in claim 4 and similarly in claim 13. Examiner's Answer, page 4. The Examiner asserts that Grawrock teaches the above-cited claim limitation. *Id.* The Examiner's reasoning for modifying Alexander with Grawrock to include the above-cited missing claim limitation is because it "provides the advantage of allowing the accurate reporting of the identity of the boot block or utility without reliance on any intervening devices (Grawrock, column 2 lines 1-6)." Examiner's Answer, page 8. The Examiner's reasoning is insufficient to establish a *prima facie* case of obviousness in rejecting claims 3-5, 7-9, 12-14 and 16-17.

The Examiner relies upon column 2, lines 1-6 of Grawrock as support for the Examiner's reasoning for modifying Alexander with Grawrock to include the above-cited missing claim limitation of claims 4 and 13. Grawrock teaches that the invention comprises the act of binding the TPM to a boot block memory device. Column 2, lines 1-3. Grawrock further teaches that this binding, which may be physical or logical through cryptographic mechanisms, allows the TPM to accurately report the identity of the boot block without reliance on any intervening devices. Column 2, lines 3-6. Hence, Grawrock teaches binding the TPM to a boot memory device which allows the TPM to accurately report the identify of the boot block without reliance on any intervening devices.

There is no language in Grawrock (and in particular column 2, lines 1-6) that makes any suggestion to verify an update to a utility by a trusted platform module (missing claim limitation) in order to accurately report the identify of the boot block without reliance on any intervening devices (Examiner's reasoning). There is no discussion of verifying an update to a utility in connection with accurately reporting the identity of the boot block. The Examiner has to provide some rational connection between the passage in Grawrock that is the source of the Examiner's reasoning and the missing claim limitation. The Examiner's source of reasoning (column 2, lines 1-6 of Grawrock) does not provide reasons as to why one skilled in the art would modify Alexander to include the missing claim limitation of claims 4 and 13. Accordingly, the Examiner has not presented a *prima facie* case of obviousness for rejecting claims 3-5, 7-9, 12-14 and 16-17. *KSR International Co. v. Teleflex Inc.*, 82 U.S.P.Q.2d 1385, 1396 (U.S. 2007); *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

Further, as stated above, in order to establish a *prima facie* case of obviousness, the Examiner must provide articulated reasoning with some rational underpinning. *KSR International Co. v. Teleflex Inc.*, 82 U.S.P.Q.2d 1385, 1396 (U.S. 2007). That is, in order to sustain the rejection of claims 4 and 13 for obviousness, the Examiner has to provide some rational connection between the Examiner's reasoning for modifying Alexander and Grawrock and the missing claim

limitation.

Alexander addresses the problem of locking critical portions of flash memory to prevent it from being corrupted during initialization as well as during normal operation of the computer system. Column 1, lines 49-57. The Examiner's rationale ("provides the advantage of allowing the accurate reporting of the identity of the boot block or utility without reliance on any intervening devices") does not provide any reasons as to why one skilled in the art would modify Alexander (which teaches resetting the flash memory to locked status without rebooting or powering down the computer system as discussed in column 1, lines 60-65) to verify an update to a utility by a trusted platform module (missing claim limitation).

Why would the reason to modify Alexander (whose purpose is to reset the flash memory to locked status without rebooting or powering down) to verify an update to a utility by a trusted platform module (missing claim limitation) be to accurately report the identity of the boot block or utility without reliance on any intervening devices (Examiner's reasoning)?

Alexander is not concerned with reporting the identity of the boot block. The Examiner cannot completely ignore the teachings of Alexander in concluding it would have been obvious to modify Alexander to include the above-cited missing claim limitation of claims 4 and 13. [1]

[1] For example, suppose that the invention of a super soaker gun (essentially a plastic gun that shoots water) was never developed and an Applicant filed for a patent application on the super soaker gun. Applicant claims a plastic gun with a container of water that shoots water. The Examiner cites a primary reference that teaches a plastic gun that shoots darts and cites a secondary reference that teaches a plastic toy that contains a container of water. Since the primary reference does not teach a container filled with water, the Examiner cites the secondary reference as teaching this missing claim limitation. The secondary reference specifically states that the purpose of the container is to carry water. The Examiner then concludes that it would have been obvious to modify the primary reference with the secondary reference in order to carry water. The Examiner believes that he/she has established a *prima facie* case of obviousness since the Examiner has found a reason to have a container of water. However, the Examiner is completely ignoring the teaching of the primary reference. Why would one skilled in the art modify a plastic gun that shoots darts to have a container of water? This is the key question to answer. While having a container of water may be used to carry water, that is irrelevant as far as the purpose of the primary reference. Simply citing to a passage in the secondary reference that discusses the purpose of that secondary reference may not be sufficient

Further, what is the rational connection between verifying an update to a utility by a trusted platform module (missing claim limitation) and accurately reporting the identity of the boot block or utility without reliance on any intervening devices (Examiner's reasoning)?

Hence, the Examiner's rationale does not provide reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would modify Alexander to include the above-cited missing claim limitation of claims 4 and 13. Accordingly, the Examiner has not presented a *prima facie* case of obviousness for rejecting claims 3-5, 7-9, 12-14 and 16-17. *KSR International Co. v. Teleflex Inc.*, 82 U.S.P.Q.2d 1385, 1396 (U.S. 2007); *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

B. Response to Examiner's interpretation of column 4, lines 9-14 of Grawrock, as discuss on page 9 of Examiner's Answer.

The Examiner asserts that the TPM of Grawrock responds to a request for verification from a challenger. Examiner's Answer, page 9. Appellants respectfully assert that the TPM of Grawrock does not respond to a request for verification from a challenger.

Grawrock teaches that the TPM 230 responds to inquiry requests from a challenger. Column 4, lines 9-10. Grawrock further teaches that a "challenger" may be any electronic device within the platform or even external to the platform. Column 4, lines 10-11. Additionally, Grawrock teaches that the "inquiry request" may be in the form of a challenge message, namely information encrypted with keying material accessible by the TPM 230. Column 4, lines 11-15. Furthermore, Grawrock teaches that in response, the TPM 230 provides TPM services such as a

---

evidence for an obviousness rejection. After all, surely there is a reason as to why the secondary reference teaches the missing claim limitation or else why would the secondary reference include it? The Examiner must explain the connection between the teachings of the primary reference and the rationale of the secondary reference for including the missing claim limitation. Otherwise, everything can be deemed obvious and virtually nothing can be patented.

digital signature featuring the boot block identifier 330, keying material, certificates and the like. Column 4, lines 15-18.

Hence, Grawrock teaches that the inquiry request from the challenger is in the form of a challenge message, namely information encrypted with keying material accessible by the TPM. Furthermore, Grawrock teaches that in response to the inquiry request from challenger, the TPM provides TPM services such as a digital signature featuring the boot block identifier, keying material, certificates and the like.

The inquiry request from the challenger is not a request for verification as asserted by the Examiner. Instead, the TPM records the operations of the boot process for subsequent verification by a challenger that the boot process occurred as expected. Column 1, lines 33-35. The challenger performs the verification not the TPM. The challenger does not send a request to the TPM for verification.

C. Response to Examiner's assertion that Alexander and Grawrock, taken in combination, teach "wherein the SMI handler used to query the status of the verifying step queries the TPM for the status" as recited in claim 5 and similarly in claim 14, as discussed on pages 10-11 of Examiner's Answer.

The Examiner cites column 5, lines 58-62 of Alexander and column 4, lines 5-19 of Grawrock as teaching "wherein the SMI handler used to query the status of the verifying step queries the TPM for the status" as recited in claim 5 and similarly in claim 14. Examiner's Answer, page 10. Appellants respectfully traverse.

Alexander teaches that when a system management interrupt (SMI) is requested, flash memory transitions from run state 304 to SMI access state 312, by first transitioning through state 340 to verify the data and state 342 to unlock flash memory 212 by outputting a reset pulse to firmware hub 110. Column 5, lines 58-62.

Hence, Alexander teaches that when a system management interrupt (SMI) is requested, the flash memory transitions from a run state to an SMI access state. Further, Alexander teaches transitioning through a state to verify the data and state to unlock the flash memory.

Grawrock teaches that the TPM 230 responds to inquiry requests from a challenger. Column 4, lines 9-10. Grawrock further teaches that a "challenger" may be any electronic device within the platform or even external to the platform. Column 4, lines 10-11. Additionally, Grawrock teaches that the "inquiry request" may be in the form of a challenge message, namely information encrypted with keying material accessible by the TPM 230. Column 4, lines 11-15. Furthermore, Grawrock teaches that in response, the TPM 230 provides TPM services such as a digital signature featuring the boot block identifier 330, keying material, certificates and the like. Column 4, lines 15-18.

Hence, Grawrock teaches that the inquiry request from the challenger is in the form of a challenge message, namely information encrypted with keying material accessible by the TPM. Furthermore, Grawrock teaches that in response to the inquiry request from challenger, the TPM provides TPM services such as a digital signature featuring the boot block identifier, keying material, certificates and the like.

There is no language in the cited passages that teaches that the SMI of Alexander (Examiner asserts that the SMI of Alexander corresponds to the SMI handler) is used to query the status of the verifying step (verifying an update to the utility). Instead, Alexander teaches that when an SMI is requested, the flash memory transitions from a run state to an SMI access state. There is no query being made as to the status of the verifying step. Neither is there any language in Grawrock that discusses a query being made as to the status of the verifying step.

Furthermore, there is no language in the cited passages that teaches that the SMI of Alexander (Examiner asserts that the SMI of Alexander corresponds to the SMI handler) used to query the status of the verifying step (verifying an update to the utility) queries the TPM for the status. There is no language in either Alexander or Grawrock that discusses querying the TPM for the status.

Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 5 and 14, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed.

Cir. 1998).

D. Response to Examiner's assertion that Examiner provided an appropriate motivation for modifying Alexander with Grawrock to include the missing claim limitation of claims 5 and 14, as discussed on pages 10 and 11 of Examiner's Answer.

As stated above, most if not all inventions arise from a combination of old elements. *See In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Obviousness is determined from the vantage point of a hypothetical person having ordinary skill in the art to which the patent pertains. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Therefore, an Examiner may often find every element of a claimed invention in the prior art. *Id.* However, identification in the prior art of each individual part claimed is insufficient to defeat patentability of the whole claimed invention. *See Id.* In order to establish a *prima facie* case of obviousness, the Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998). The Examiner must provide articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (cited approvingly in *KSR International Co. v. Teleflex Inc.*, 82 U.S.P.Q.2d 1385, 1396 (U.S. 2007)).

The Examiner admits that Alexander does not teach the aspect of querying the TPM for the status of the verifying step, as recited in claim 5 and similarly in claim 14. Examiner's Answer, page 10. The Examiner asserts that Grawrock teaches the above-cited claim limitation. *Id.* The Examiner's reasoning for modifying Alexander with Grawrock to include the above-cited missing claim limitation is because it "provides the advantage of allowing the accurate reporting of the identity of the boot block or utility without reliance on any intervening devices (Grawrock, column 2 lines 1-6)." Examiner's Answer, pages 10-11. The Examiner's reasoning is insufficient to establish a *prima facie* case of obviousness in rejecting claims 5 and

14.

The Examiner relies upon column 2, lines 1-6 of Grawrock as support for the Examiner's reasoning for modifying Alexander with Grawrock to include the above-cited missing claim limitation of claims 5 and 14. Grawrock teaches that the invention comprises the act of binding the TPM to a boot block memory device. Column 2, lines 1-3. Grawrock further teaches that this binding, which may be physical or logical through cryptographic mechanisms, allows the TPM to accurately report the identity of the boot block without reliance on any intervening devices. Column 2, lines 3-6. Hence, Grawrock teaches binding the TPM to a boot memory device which allows the TPM to accurately report the identify of the boot block without reliance on any intervening devices.

There is no language in Grawrock (and in particular column 2, lines 1-6) that makes any suggestion to query the TPM for the status of the verifying step (missing claim limitation) in order to accurately report the identify of the boot block without reliance on any intervening devices (Examiner's reasoning). There is no discussion of querying the TPM for the status of the verifying step (verifying an update to a utility) in connection with accurately reporting the identity of the boot block. The Examiner has to provide some rational connection between the passage in Grawrock that is the source of the Examiner's reasoning and the missing claim limitation. The Examiner's source of reasoning (column 2, lines 1-6 of Grawrock) does not provide reasons as to why one skilled in the art would modify Alexander to include the missing claim limitation of claims 5 and 14. Accordingly, the Examiner has not presented a *prima facie* case of obviousness for rejecting claims 5 and 14. *KSR International Co. v. Teleflex Inc.*, 82 U.S.P.Q.2d 1385, 1396 (U.S. 2007); *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

Further, as stated above, in order to establish a *prima facie* case of obviousness, the Examiner must provide articulated reasoning with some rational underpinning. *KSR International Co. v. Teleflex Inc.*, 82 U.S.P.Q.2d 1385, 1396 (U.S. 2007). That is, in order to sustain the rejection of claims 5 and 14 for

obviousness, the Examiner has to provide some rational connection between the Examiner's reasoning for modifying Alexander and Grawrock and the missing claim limitation.

Alexander addresses the problem of locking critical portions of flash memory to prevent it from being corrupted during initialization as well as during normal operation of the computer system. Column 1, lines 49-57. The Examiner's rationale ("provides the advantage of allowing the accurate reporting of the identity of the boot block or utility without reliance on any intervening devices") does not provide any reasons as to why one skilled in the art would modify Alexander (which teaches resetting flash memory to locked status without rebooting or powering down the computer system as discussed in column 1, lines 60-65) to query the TPM for the status of the verifying step (verifying an update to a utility) (missing claim limitation).

Why would the reason to modify Alexander (whose purpose is to reset the flash memory to locked status without rebooting or powering down) to query the TPM for the status of the verifying step (missing claim limitation) be to accurately report the identity of the boot block or utility without reliance on any intervening devices (Examiner's reasoning)?

Alexander is not concerned with querying a TPM for a status. The Examiner cannot completely ignore the teachings of Alexander in concluding it would have been obvious to modify Alexander to include the above-cited missing claim limitation of claims 5 and 14.

Further, what is the rational connection between querying the TPM for the status of the verifying step (missing claim limitation) and accurately reporting the identity of the boot block or utility without reliance on any intervening devices (Examiner's reasoning)?

Hence, the Examiner's rationale does not provide reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would modify Alexander to include the above-cited missing

claim limitation of claims 5 and 14. Accordingly, the Examiner has not presented a *prima facie* case of obviousness for rejecting claims 5 and 14. *KSR International Co. v. Teleflex Inc.*, 82 U.S.P.Q.2d 1385, 1396 (U.S. 2007); *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

E. Response to Examiner's assertion that Alexander teaches "if the verifying step successfully verifies the update of the utility, unlocking the utility and updating the utility," as recited in claim 4 and similarly in claim 13, as discussed on page 11 of Examiner's Answer.

The Examiner cites column 5, lines 41-45 and 58-67 of Alexander as teaching "if the verifying step successfully verifies the update of the utility, unlocking the utility and updating the utility," as recited in claim 4 and similarly in claim 13. Examiner's Answer, page 11. Appellants respectfully traverse.

Alexander teaches that control is then transferred to state 336 where BIOS 142 puts all protected blocks in firmware hub 110 in locked status before passing control to computer system's 100 operating system and entering run state 304. Column 5, lines 39-42. Alexander further teaches that if a valid RBU image exists, flash memory 212 enters state 338 where BIOS 142 updates firmware hub 110 with a new BIOS image and then enters state 302 to load the new image by resetting computer system 100. Column 5, lines 42-46. Additionally, Alexander teaches when a system management interrupt (SMI) is requested, flash memory transitions from run state 304 to state SMI access state 312, by first transitioning through state 340 to verify the data and state 342 to unlock flash memory 212 by outputting a reset pulse to firmware hub 110. Column 5, lines 58-62. In addition, Alexander teaches that once the SMI handler updates the requested information successfully, control transitions to state 344 to lock flash memory 212. Column 5, lines 62-64. Furthermore, Alexander teaches that if an error occurs in attempting to update the information, control transitions to state 346 where an error code is set and then to state 344 to lock flash memory 212. Column 5, lines 64-67.

Hence, Alexander teaches that the flash memory enters state 338 where the BIOS updates the firmware hub with a new BIOS image and then enters state 302 to

load the new image by resetting the computer system. Furthermore, Alexander teaches that when a system management interrupt (SMI) is requested, the flash memory transitions from a run state to an SMI access state by transitioning through state 340 to verify the data and state to unlock the flash memory. Additionally, Alexander teaches that once the SMI handler updates the requested information successfully, control transitions to state 344 to lock the flash memory.

The Examiner cites to the flash memory of Alexander as teaching the claimed utility. Examiner's Answer, page 11. There is no language in the cited passages that teaches that if the verifying step successfully verifies the update of the utility, unlocking the utility (Examiner asserts that the flash memory of Alexander teaches the claimed utility) and updating the utility. Instead, the cited passages teach that once the SMI handler updates the requested information successfully, the flash memory is locked. This is the opposite of unlocking the utility.

Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 4 and 13, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Furthermore, the Examiner cites to column 5, lines 9-18 and 57-67 of Alexander in support of the assertion that Alexander teaches unlocking the utility and updating the utility if the verifying step successfully verifies the update of the utility. Examiner's Answer, page 12. Appellants respectfully traverse.

Alexander teaches that when an update to BIOS 142 is requested from a remote application or operating system instruction, flash memory enters remote BIOS update (RBU) state 306. Column 5, lines 11-13. Furthermore, Alexander teaches that when the update is complete, computer system 100 passes control from RBU state 306 to power on reset state 302 to perform the power on self test, resets all blocks in flash memory 212 to locked status, and passes control to run state 304. Column 5, lines 13-17.

Hence, Alexander teaches that when an update to the BIOS is requested from

a remote application or operating system instruction, the flash memory enters a state known as the remote BIOS update state. Alexander further teaches that the computer system passes control from the remote BIOS update state to the power on reset state to reset all the blocks in the flash memory to the locked status.

There is no language in the cited passage that teaches unlocking the flash memory (Examiner asserts that the flash memory of Alexander teaches the claimed utility) if the verifying step successfully verifies the update of the flash memory. Instead, Alexander teaches that once the flash memory enters the remote BIOS update state, the computer system passes control to the power on reset state to reset all the blocks in the flash memory to the locked status.

Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 4 and 13, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Furthermore, as stated above, column 5, lines 57-67 of Alexander teaches that when a system management interrupt (SMI) is requested, the flash memory transitions from a run state to an SMI access state by transitioning through state 340 to verify the data and state to unlock the flash memory. Additionally, Alexander teaches that once the SMI handler updates the requested information successfully, control transitions to state 344 to lock the flash memory.

There is no language in the cited passage that teaches that if the verifying step successfully verifies the update of the utility, unlocking the utility (Examiner asserts that the flash memory of Alexander teaches the claimed utility) and updating the utility. Instead, the cited passages teach that once the SMI handler updates the requested information successfully, the flash memory is locked. This is the opposite of unlocking the utility.

Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 4 and 13, since the Examiner is relying upon incorrect, factual predicates in support of the rejection. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed.

Cir. 1998).

F. Other matters raised by the Examiner.

All other matters raised by the Examiner have been adequately addressed above and in Appellants' Appeal Brief (7/22/2009) and therefore will not be addressed herein for the sake of brevity.

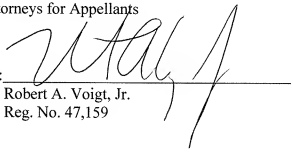
II. CONCLUSION:

For the reasons stated above and in Appellants' Appeal Brief (7/22/2009), Appellants respectfully assert that the rejections of claims 3-5, 7-9, 12-14 and 16-18 are in error. Appellants respectfully request reversal of the rejections and allowance of claims 3-9 and 12-19.

Respectfully submitted,

WINSTEAD P.C.

Attorneys for Appellants

By: 

Robert A. Voigt, Jr.
Reg. No. 47,159

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2832

Austin_1 585723v.1